Research and Application of Multi-chain Sharing Architecture of Electronic License

Wenhao Xue[1,3(✉)], Fan Jia[2,4], Huanjuan Wang[1], Jiangtao Li[2], and Guomin Li[3]

[1] State Grid Blockchain Technology (Beijing) Co., Ltd., Beijing, China
slam_hao@163.com.cn, wanghuanjuan@sgec.sgcc.som.cn
[2] State Grid Blockchain Technology Laboratory, Beijing, China
{jiafan,lijiangtao}@sgec.sgcc.som.cn
[3] State Grid Digital Technology Holding Co., Beijing, China
liguomin@sgec.sgcc.som.cn
[4] State Grid Xiongan Financial Technology Co., Beijing, China

Abstract. In order to solve the pain points of the traditional paper license offline business, such as the large number of communication units and cumbersome work, under the strong advocacy and development of the state, the electronic licenses came into being, which greatly reduces the complexity of the offline business. However, in the face of large-scale and highly concurrent electronic licenses requests, the efficient sharing scheme of electronic licenses information, sharing efficiency guarantee, security authority control of electronic licenses and other aspects need to be further studied and optimized. This paper proposes a Inter-Blockchain electronic licenses-sharing architecture based on blockchain, which adapts to the electronic licenses data sharing under the multi-chain mode. At the same time, it controls the security and reliability of license access information based on smart contracts, comprehensively guarantees the efficient sharing of electronic licenses information among multiple departments, and helps create a good application ecology of electronic licenses.

Keywords: blockchain · electronic license · Inter-Blockchain

1 Introduction

With The State Council issued "on accelerating the promotion of the" Internet + government services "work guidance", to accelerate the promotion of government information data sharing, accelerate the realization of electronic licenses library and electronic licenses management system. However, most provinces or industries independently manage their own electronic licenses at present. In the examination of electronic licenses, application, transmission, verification and other operations need to be carried out through the interaction between different electronic licenses libraries. The sharing process and links are complicated, and have high requirements on the response speed and communication stability of each system. When there is a high number of concurrent requests, the central system is under great pressure cause request timeout, service downtime and

J. Yen et al. (Eds.): ICBIS 2023, AHCS 14, pp. 1189–1195, 2023.
https://doi.org/10.2991/978-94-6463-198-2_123

other problems, the sharing efficiency of electronic licensess is affected. Blockchain technology has the characteristics of "non-forgery", "full traces", "traceable", "open and transparent", "collective maintenance", etc., which can fully guarantee the authenticity in the sharing process of electronic licensess and licenses and the sharing efficiency of multi-party endorsement.

This paper proposes an electronic licenses-sharing mode based on multi-chain architecture. By linking the license information of various electronic licenses libraries to the subject blockchain, various electronic licenses of various departments and regions are unified and abstracted, and all chains interact with each other in the form of Inter-Blockchain, so as to provide universal trusted verification, trusted sharing and whole-process traceability services. Play the role of blockchain in promoting license-sharing, optimizing business processes, reducing operating costs, and improving collaborative efficiency, overcoming the problems of traditional electronic licenses network communication obstruction, strict access control, cumbersome verification process and so on, improving the speed of license-sharing and verification efficiency, and lay a solid foundation for the construction of high technology of electric power network with mutual trust and efficient collaborative development. Fully respond to the national strategic call of “One Network Access”, realize the circulation of license information across provinces, cities and departments, and create a certificate service system of One Network Access [1].

2 Electronic License Multi-chain Sharing Architecture

This paper mainly constructs a multi-chain sharing architecture of electronic licensess based on blockchain. The core method is that multiple nodes of a certain subject’s blockchain jointly save the electronic licensess information. When the business system initiates the electronic licensess inspection demand, it initiates a sharing request to the blockchain. The advantages of this license-sharing scheme lie in three aspects: one is multi-node endorsement, which can guarantee the authenticity and verifiability in the sharing process of electronic licenses; the other is multi-node communication guarantee, which increases the verification channel, and can allocate transactions to different nodes for processing after receiving a large number of requests, so as to avoid emergencies such as long service queue and slow response speed. Third, electronic licenses-sharing based on blockchain can record and trace the operation behaviors and data in the whole process of invoking license, comprehensively improving the stability and security in the process of electronic licenses-sharing [2, 3]. The structure of block chain-based electronic licensess is shown in Fig. 1

The multi-chain sharing architecture of the e-license is mainly composed of the chain of custody, each business chain and Inter-Blockchain gateway, which supports the Inter-Blockchain data and behaviors of the e-license and guarantees the efficient sharing and verification of the e-license.

1. The chain of custody is mainly composed of the national or industrial blockchain or master node, which acts as the supervisor of the electronic licenses-sharing process to ensure the compliance sharing and whole-process supervision of the electronic licenses.

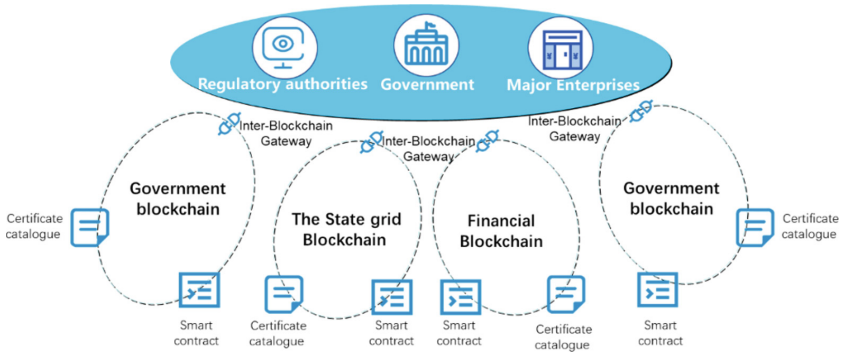

Fig. 1. Multi-chain sharing architecture of electronic license

2. Business chain refers to the blockchain platform corresponding to each electronic licenses library. The scheme described in this paper is compatible with various blockchain technical architectures. Various license libraries will encrypt the license information onto the chain and form a license catalog to provide basic data support for Inter-Blockchain.
3. The Inter-Blockchain gateway is responsible for the verification, persistence and routing of Inter-Blockchain messages between various business chains, and provides functions such as collection, analysis of Inter-Blockchain transactions and message forwarding of Inter-Blockchain transactions.

3 Electronic License Multi-chain Inter-blockchain Sharing Scheme

Inter-Blockchain sharing of electronic licensess and licenses based on blockchain mainly includes the following steps: [4, 5] and the electronic license Inter-Blockchain process is shown in Fig. 2.

- Business system users send electronic licenses-sharing requirements to business chain 1;
- Nodes in business chain 1 verify the sharing requirements of users' electronic licensess and licenses, and persist them to the block of business chain 1 through consensus;
- The Inter-Blockchain gateway captures the e-license Inter-Blockchain event on the service chain 1, analyzes the Inter-Blockchain event, encapsulates the Inter-Blockchain message, and routes it to the target Inter-Blockchain gateway;
- The target cross-link gateway first carries out data verification and existence verification for the shared message, and stores the e-license shared message to service chain 2 after the verification is passed;
- Business chain 2 Perform the corresponding Inter-Blockchain sharing operation, and reverse the sharing receipt information to perform the above process.

Inter-Blockchain gateway needs to verify every Inter-Blockchain transaction to prevent the transaction from being forged or tampered with. The verification engine is implemented in a plug-in way, which can deal with the verification of its own rules by

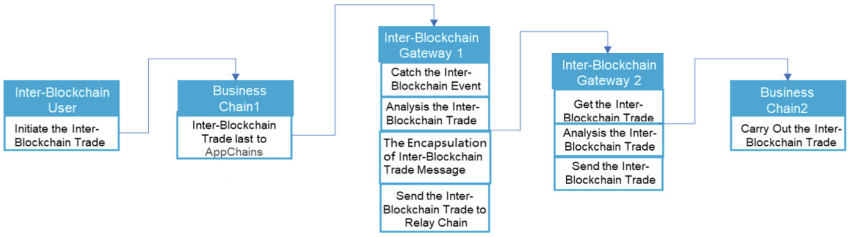

Fig. 2. Electronic license Inter-Blockchain process

various types of blockchain, and can support online upgrade and transformation, which can deal with and manage a variety of complex logic verification rules.

When the service chain needs to be cross-linked, events are thrown, and then the Inter-Blockchain gateway encapsulates the Inter-Blockchain transaction. The Inter-Blockchain gateway needs to verify each Inter-Blockchain transaction to prevent the transaction from being forged or tampered. The verification engine is implemented in a plug-in way, which can deal with the verification of its own rules by various types of blockchain, and can support online upgrade and transformation, which can deal with and manage a variety of complex logic verification rules.

The routing module can route Inter-Blockchain transactions and their returns. After Inter-Blockchain transaction verification is passed, all Inter-Blockchain transactions to be routed in a block are constructed into a Merkle Tree. The Merkle Root is either sent to the destination chain for execution after the signature of the verified node or to the next hop, another Inter-Blockchain gateway. When sending to another Inter-Blockchain gateway, the verifiable data structure and signature of the Inter-Blockchain gateway need to be added in the Proof field so as to verify the reliability of the Inter-Blockchain transaction at the next hop.

4 Electronic License Authority Control Mechanism

Combined with the electronic licenses-sharing and management scenario, this paper proposes a fine-grained access control model based on blockchain smart contracts [6, 7]. By writing corresponding access control modules inside the smart contracts [8], it realizes the permission management for different roles to access data resources of different secret levels. There are two main functions involved.

- Set different user roles for electronic licenses data resources of different secret levels to form a hierarchical access control mechanism for data resource secret level attributes
- Set the dynamic permission control module to realize the dynamic granting and recycling of temporary access permission of users to certain secret level electronic licenses resources.

The main idea of this method is Based on the review and assessment of user identity and responsibilities, user roles are assigned corresponding access rights. The execution framework and workflow of access control smart contracts are as follows. Smart Contract Authority control scheme is shown in Fig. 3.

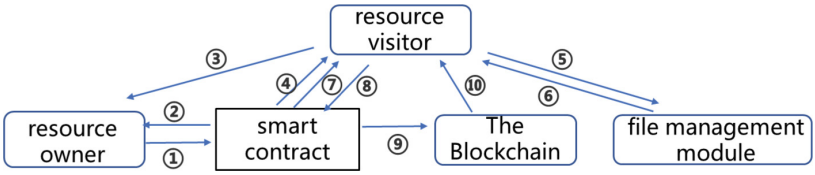

Fig. 3. Smart Contract Authority control scheme

The simple workflow for access control consists of the following 10 steps:

1. The e-license resource owner uses the contracts management module to deploy or call the interface function in the contracts;
2. The owner of the electronic licenses resource gets the feedback result of the operation;
3. When the electronic licenses resource visitor sends the authorization request, it calls the permission management function in the smart contracts through the contracts module;
4. Assign the role and authority to the electronic licenses resource visitor through the rights management function inside the contracts, and write it into the permission set;
5. 5 When the visitor to the electronic licenses resource needs to access a certain file, it can obtain the file number, secret level and smart contracts access address of the unit through the off-chain file management module;
6. Obtain the smart contracts address and file number through Step 5, and invoke the interface function of the electronic licenses resource to be accessed within the contracts through the contracts address;
7. In the smart contracts, the user accesses the permission set inside the contracts according to the established logic, and checks whether the user's permission record exists through the account address of the current user.
8. Obtain the query permission result. If the current permission set has the permission record of the user, the user role and corresponding user permissions of the current electronic licenses resource visitor are obtained, go to Step 9; otherwise, go to Step 10.
9. Access the electronic licenses resource set that stores the confidential files according to the secret level of the electronic licenses resource;
10. The visitor of electronic licenses resource obtains the access result and judges the size of the file according to the obtained file information. The electronic licenses resource with large capacity is accessed through the hash address of the obtained data resource, while the electronic licenses resource with small capacity is directly obtained from the information.

Table 1. Blockchain license information table

Certificate No.	Settlement deposit No.	Contract deposit No.	Electronic certificate fingerprint
1220014145	af2b211cd05b289a16b98803869bf89016cf7afd035ab44450169b8079df8ea0	1ea964bace1775dcd9e974059eaecc9c4bf5dcc272e0784f304c7c6b4bcff5ac	9cf03e4e2d4f0eabf8ff1cf9e11b7ee01c08c2c90050ede4f3f85d20437b3a17
1220014146	49632fecc1e55e075820d8ca7c959c21e1503179716244b5ac2b200d2b17ec94	8f785ef2e881a33227608eda65890ee88251e9f5d2530b6fb307f3e727a16aa4	41b8ecdc6671797510948ec4a37d64d627ef9d33056b60df1c814f9e3bddc440
1220014147	ea9777171442b438df680cb86a4623548f2b8dea617fe26c710f9f0d26166690	b5d501c3b4ff53f0970a131786ee61f3d5be7f9a7be8c310cd03a35c6fd5933c	e642c8292f71437d220425a7237a8174961fe047d0d9ed1af663ef5f16cac020

5 Experiment and Verification

In this paper, two blockchains A and B are constructed in the experimental environment. The corresponding electronic licenses library and business system are supported under the chain. This experiment is carried out with the green power transaction voucher busines. First, issue green power transaction vouchers on the business system associated with A-chain, form a list of green power transaction electronic licenses directories, use SM3 algorithm to generate hash fingerprints of vouchers, and record the original text of the directory and the file fingerprints of all vouchers in A-chain.

In the experimental environment, when the user uses and verifies the certificate in a business system associated with the B-chain, user enters the key field of the certificate in the business system and uploads the certificate to initiate the verification. After receiving the request, the business system uploads the original text of the key field entered by the user and the certificate to the blockchain through the hash converted by the SM3 algorithm, and the information is Inter-Blockchain to the business chain A based on the cross-link gateway, Chain A uses a smart contracts to compare the Inter-Blockchain data with the previously backed up electronic licenses index table. After the verification is consistent, it sends back the correct information for business chain B through the Inter-Blockchain method. Business chain B returns the verification results to the business system. The verification is successful and the verification is completed. Table 1 is the block information recorded on the A-chain.

6 Conclusion

As a new direction for the development of social services, efficient and secure sharing of electronic licensess is an important guarantee means for this business. This paper proposes a solution that adapts to the high concurrency and large-scale sharing of licenses

through the design of electronic licenses-sharing architecture, license information sharing based on Inter-Blockchain technology and security control of electronic licenses-sharing. To provide more convenient solution conditions for the development of the e-license business, fully support the application and expansion of the e-license, and fully help the implementation of the strategic deployment of the "All Access Office".

Acknowledgements. This work is supported by the SGDT Science and Technology Project "Research and application of key technologies of blockchain in electronic certificates," Funding, Project No.: 1200/2022-72003B.

References

1. Cui Z, Fei X U E, et al. A hybrid blockchain-based identity authentication scheme for multi-WSN[J]. IEEE Transactions on Services Computing, 2020, 13(2): 241-251.
2. Rouhani S, Butterworth L,et al. MediChain TM: a secure decentralized medical data asset management system[C]//2018 IEEE International Conference on Internet of Things (i Things) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Canada, IEEE, 2018: 1533–1538.
3. Min Xurong, Du Kui, Dai Yicong. Design of electronic certificate sharing platform based on blockchain technology [J]. Command Information System and Technolo-gy,2017,8(02):47-51.DOI:https://doi.org/10.15908/j.cnki.cist.2017.02.009
4. Qiu H . METHOD AND APPARATUS FOR INTER-BLOCKCHAIN TRANSMISSION OF AUTHENTICABLE MESSAGE:, US20200366486A1[P]. 2020.
5. Li Fang, Li Zhuoran, Zhao He. Research on the progress of blockchain Inter-Blockchain technology [J]. Journal of Software,2019,30(06):1649-1660.DOI:https://doi.org/10.13328/j.cnki.jos.005741
6. Jorstad I. Strong authentication for services with mobile universal identity[C]. International Conference on Mobile Web and Information Systems. Springer, Cham, 2022: 27–36.
7. Ma J, Liu J, Huang X, et.al. Authenticated Data Redaction with Fine-Grained Control[J]. IEEE Transactions on Emerging Topics in Computing,2020,8(2): 291-302.
8. Rouhani S, Deters R. Blockchain based access control systems: State of the art and challenges